RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: LAW-M05

Hot!
Sizzling Cyber Law Topics

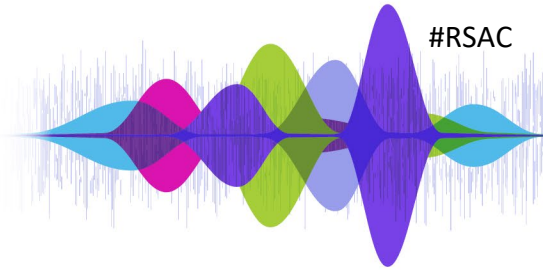
MODERATOR: **Ruth Hill Bro**
Privacy and Cybersecurity Attorney

PANELISTS: **Ted Claypoole**
Partner
Womble Bond Dickinson (US) LLP

Kristin J. Madigan
Partner
Crowell & Moring

Lucy L. Thomson
Principal
Livingston PLLC

Disclaimer



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

#RSAC

Many Voices.
One Community.

MODERATOR:

Ruth Hill Bro

Privacy and Cybersecurity Attorney

https://www.linkedin.com/in/ruth-hill-bro-4723622/

PANELISTS:

Ted Claypoole

Partner
Womble Bond Dickinson (US) LLP

https://www.linkedin.com/in/tedclaypoole/

Kristin J. Madigan

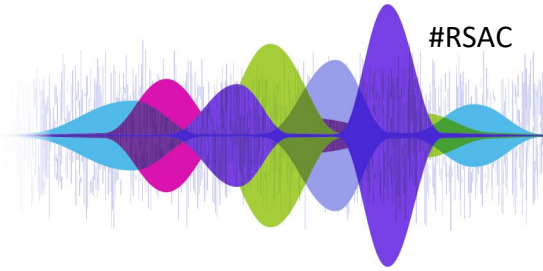
Partner
Crowell & Moring

https://www.linkedin.com/in/kristin-madigan-cipp-us-7a627982/

Lucy L. Thomson

Principal
Livingston PLLC

https://www.linkedin.com/in/lucylivingstonthomson/



Agenda (Hot! Topics)

1. Prying eyes (surveillance pricing, drones, and more) – Ruth
2. AI hologram rights & wrongs – Ted
3. AI developers in regulatory spotlight – Lucy
4. FTC, SEC, & DOJ spell trouble for AI washing – Kristin
5. The rise of neuro privacy (I know what you thought last summer) – Ted
6. Software supply chain compromises (third-party ripple effects) – Lucy
7. Cyber post-Chevron – Kristin
8. *Takeaways, Resources, and Q&A – All*

Topic 1: Prying Eyes

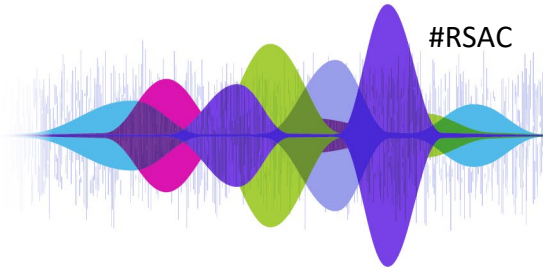
Music:

- “Private eyes, they’re watching you, they see your every move” (1981)
- ”I am the eye in the sky, looking at you, I can read your mind” (1982)
- “Every step you take, every move you make … I’ll be watching you” (1983)
- “I always feel like somebody’s watching me, and I have no privacy” (1984)

Fiction/Film (book, movie):

- “Big Brother is watching you” (1949, 1984)
- Eye of Sauron/Great Eye (1954, 2001)
- Minority Report (1956, 2002)

Tracking: Real-Life Warnings



Samuel Warren/Louis Brandeis in *Harvard Law Review* on "The Right to Privacy" in **1890**

Discussing threats to what Judge Cooley described as the right "to be let alone" so that "… what is whispered in the closet shall be proclaimed from the house-tops."

Sun Microsystems CEO Scott McNealy in 1999:

"You have zero privacy anyway. Get over it."

Former NSA contractor/leaker Edward Snowden in 2013:

"We have sensors in our pockets that track us everywhere we go…. A child born today will grow up with no conception of privacy at all. They'll never know what it means to have a private moment to themselves – an unrecorded, unanalyzed thought. And that's a problem because privacy matters; privacy is what allows us to determine who we want to be."

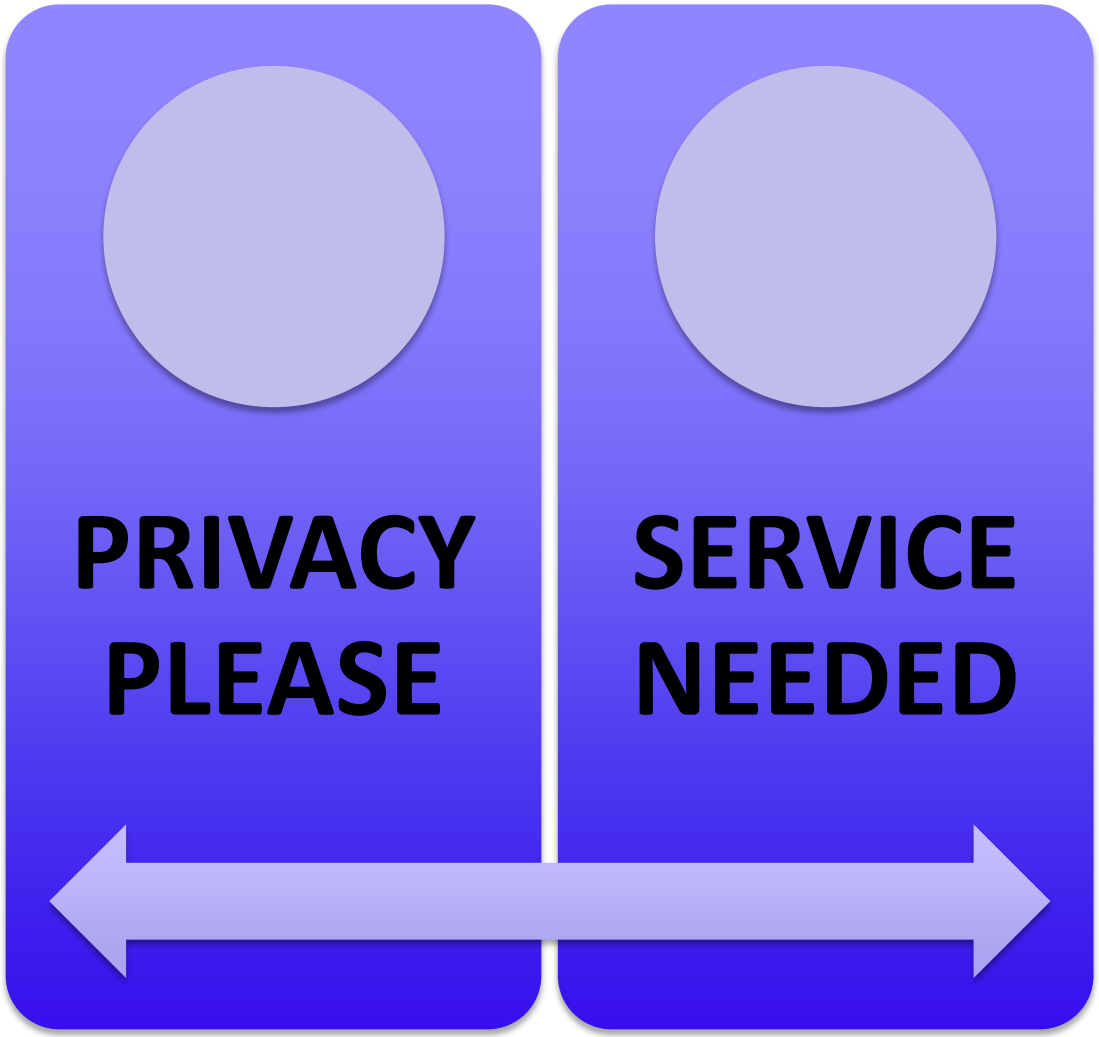
Prying Eyes: Technology (BAD?)

- **Biometrics** – Biologically unique to individual (retina & iris scans, fingerprints, voiceprints, scans of hand or face geometry). Thus highly personal and poses unique risks. Unlike SSN, biometric data can't be changed.
  - Laws: Biometrics laws in IL, TX, WA; states like AZ include biometric data in definition of personal information in their security laws; laws can be at city level (eg, NYC); global reach (eg, EU AI Act)
- **AI –** AI systems rely on personal data, online communications, images and video depicting people, etc. to train algorithms, enhance performance, process input, and deliver output.
  - In daily life: open phones with face ID (machine learning algorithms), get personalized social media feeds, read email, use search engines, use digital voice assistants, get travel directions, do online banking, use smart home devices
  - With customers: provide highly targeted marketing (and pricing), customer-focused recommendations, virtual customer assistance, etc.
  - With employees: make decisions and predictions about employees, customize automated training, assess and increase productivity, minimize mistakes and safety hazards
- **Drones –** autonomous deliveries to customers, inventory and facilities management, warfare, and
  - Insurance: Inspect properties; identify risks (roof, trees); assess storm damage; deny, renew, or cancel coverage; etc.
  - Drone as first responder (DFR): get there first (act as eyes and ears), improve response times and search, enhance safety … but also privacy concerns
  - Drone journalism: 5th Circuit upheld Texas law, *Nat'l Press Photographers Ass'n v. McCraw*, 90 F.4th 770 (5th Cir. 2024)

Prying Eyes: Legal Developments

- **Government:** 18 State AGs filed 2/7/25 lawsuit to stop new Administration's unauthorized disclosure of Americans' private info./sensitive data (Treasury).
- **Private sector:**
  - FTC used 6(b) authority to study "surveillance pricing," sent orders to 8 companies using algorithms/AI and personal data to categorize people and set personal prices for the same goods/services 7/23/24
  - Surveillance capitalism complaints/lawsuits:
    - *Kolotinsky v Amazon.com* (N.D. Cal., No. 3:25-cv-00931, complaint 1/29/25)
    - *Roque v. Allstate* (N.D. Ill., No. 1:25-cv-00709, complaint 1/25/25)
    - *Atkins v. Amplitude* (N.D. Cal., No. 3:24-cv-04913, complaint 8/8/24)
    - *FTC v. Kochava* (second amended complaint 7/15/24)
  - Stadiums as the future of surveillance? Airports, theme parks, office & apartment buildings, hotels, rideshare, public transportation, banks, stores, restaurants, schools, medical offices…
- **A universal identity platform?** "CLEAR" privacy/security implications

Apply to Practice



- It’s like those hotel room door tags … build trust
  - Disclose practices
  - Keep promises
  - Use data for needed services

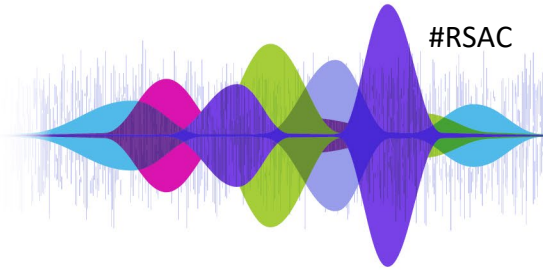
Topic 2: AI Hologram Rights and Wrongs

Elvis Evolution: London May 2025

Pre-Generative AI

- What laws might have applied?
  - Commercial **unfair and deceptive practices** laws
  - **Trademarks** in some cases
  - **Copyright** protection for songs and performances
  - State laws protecting **name, image, and likeness**
    - Inconsistent
    - Patchy coverage

Laws Targeting *Results* of AI, Not *Use* of AI



- **Colorado** AI law doesn't apply here
  - Protect individuals from algorithmic discrimination by artificial intelligence systems operating in Colorado
- **EU Act** probably doesn't apply here
  - Deepfakes not specifically called out as prohibited
  - Mostly applying to AI affecting or manipulating people

Tennessee Ensuring Likeness Voice and Image Security Act

- **ELVIS Act**
  - Prohibits cloning the voice of an artist (audio deepfakes)
  - Class A misdemeanor
  - Adds voice to pre-existing property right in name, photo, or likeness
  - Voice is “a sound in a medium that is readily identifiable and attributable to a particular individual, regardless of whether the sound contains the actual voice or a simulation of the voice of the individual”
  - Fair use exemptions, including fleeting and incidental use

California Cascade of AI Laws

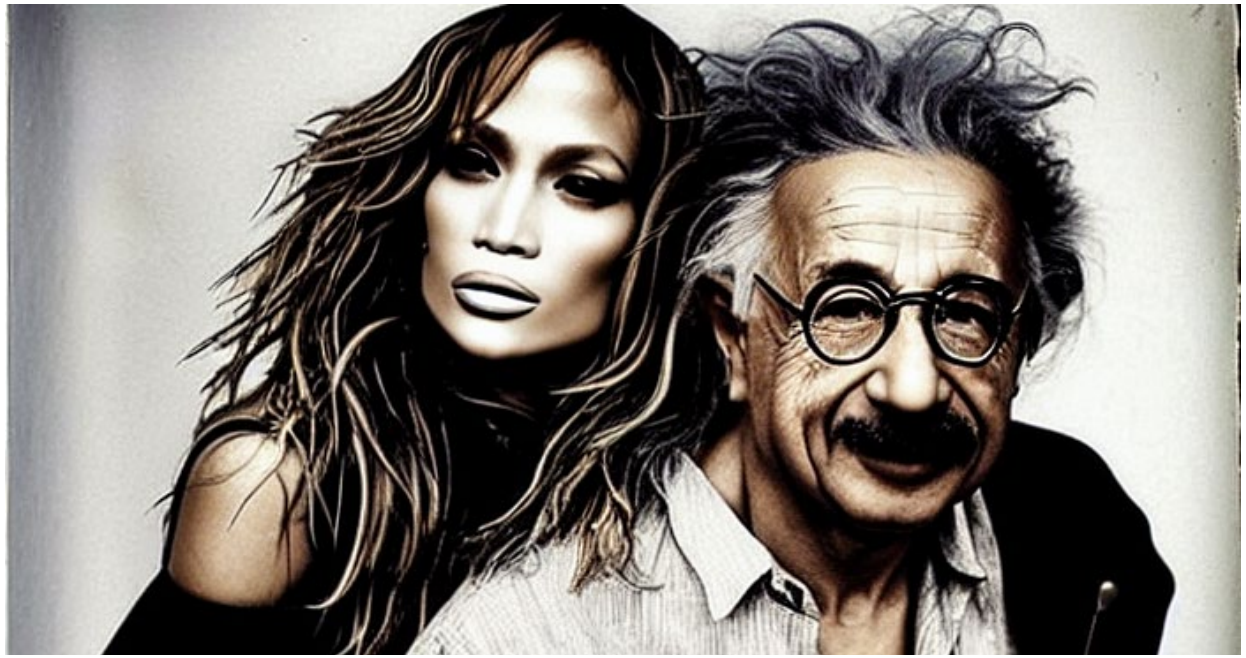
- Assembly Bill No. 2602
  - Contracts allowing digital likeness of individual are unenforceable starting in 2025
  - Visual likeness of an individual
    - that is embodied in a sound recording, image, audiovisual work, or
    - transmission in which the actual individual either did not actually perform or appear, or
    - the actual individual did perform or appear, but the fundamental character of the performance or appearance has been materially altered.
  - Fine for film 🎥 … what about video games 🎮?

California Cascade of AI Laws

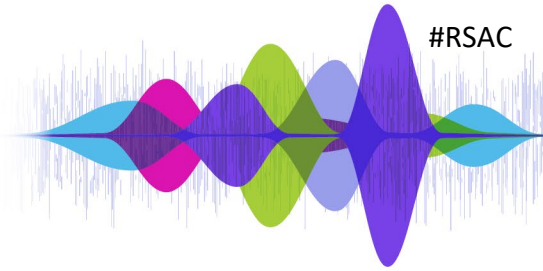
- Assembly Bill No. 1836
  - Prevents production or distribution of “the digital replica of a deceased personality’s voice or likeness in an expressive audiovisual work or sound recording without specified prior consent”
  - Ends 70 years after death of person
  - **Digital replica** means “a computer-generated, highly realistic electronic representation that is
    - readily identifiable as the voice or visual likeness of an individual that is embodied in a sound recording, image, audiovisual work, or
    - transmission in which the actual individual either did not actually perform or appear, or
    - the actual individual did perform or appear, but the fundamental character of the performance or appearance has been materially altered.

Apply to Practice

- States are already limiting un-consented use of image, voice, likeness
  - Either use long-dead famous people, or request permission
  - Hologram shows are particularly vulnerable – voice and likeness
  - We will likely see more protections against deepfakes and digital likenesses



Topic 3:
AI Developers in Regulatory Spotlight



New State AI laws

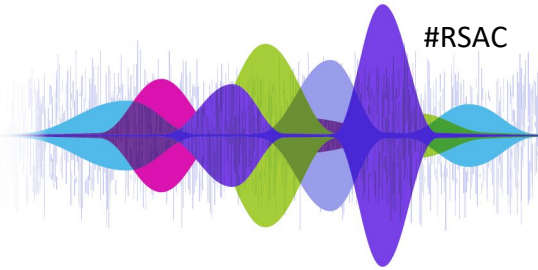
Create obligations on participants throughout the AI ecosystem, from designers to users

- **COLORADO** (eff. Feb. 2026) – requires developers and deployers of high-risk AI systems to use reasonable care to protect consumers from risks of algorithmic discrimination
  - Requires adoption of risk management policy, impact assessment, annual review, and consumer rights notification
- **ILLINOIS** (eff. Jan. 2026) – Prohibits employers from using AI in employment decisions if they have a discriminatory effect
  - Requires employers to notify employees of AI usage

AI Developers in the Regulatory Spotlight

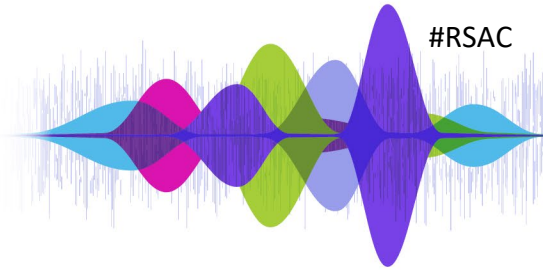
- **European Union AI Act**
  - **Risk-based approach defines four levels of AI risk:** unacceptable risk, high risk, minimal/limited risk, and specific transparency risk.
  - AI developers must ensure **high-risk AI systems** comply with strict obligations, including risk assessment, data quality, logging, documentation, and human oversight; general-purpose AI models have transparency obligations and potential systemic risk evaluations.
- **ABA AI Guidelines** (Resolution 604 (2023))
  - **"Developers"** should ensure their AI products, services, systems, and capabilities are subject to human authority, oversight, and control, and provide accountability and transparency for AI.

Apply to Practice



- Be careful with high-risk systems and data
- Use the NIST AI Risk Management Framework to identify and manage the risks
- Ensure that there are humans in control, not just in the loop

Topic 4: FTC, SEC, and DOJ Spell TROUBLE for AI Washing



FTC

Operation AI Comply

September 2024: FTC announced 5 law enforcement actions against firms that use AI hype or sell AI tech that can be used in deceptive or unfair ways:

- Do Not Pay
- Ascend Ecom
- Ecommerce Empire Builders
- Rytr
- FBA Machine

SEC

March 2024: Recent enforcement actions highlighting AI risks and increased scrutiny of AI-related disclosures

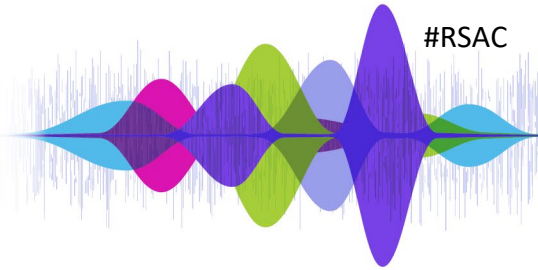
- Global Predictions, Inc. + Delphia (USA) Inc.
- Alleged false statements re use of AI
- Agreed to settle SEC charges and pay $400,000 in total civil penalties

DOJ

September 2024: Criminal division issued an updated Evaluation of Corporate Compliance Programs (ECCP)

- Emphasizes that companies should address risks associated with new technologies, such as AI
- Highlights the importance of incentivizing and protecting whistleblowers

The Current Federal Approach to AI



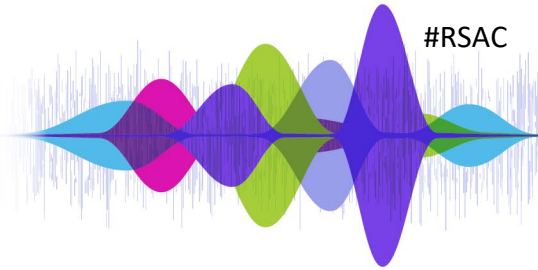
- **January 20, 2025**
  - President Trump revoked Executive Order 14110: “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence”
- **February 6, 2025**
  - The National Science Foundation (NSF) released an RFI to solicit public input for a national AI Action Plan
- **U.S. states** have taken a much more active role in proposing and enacting AI legislation

Apply to Practice

- Re federal regulation and enforcement around AI claims
  - Anticipate skepticism for novel interpretation of existing federal law or edge cases
  - States will likely continue to outpace the feds
  - AI claims made to consumers, however, will continue to be scrutinized at the federal level, depending on their nature and context

Topic 5: The Rise of Neuro Privacy

Brain Processes and Access Devices



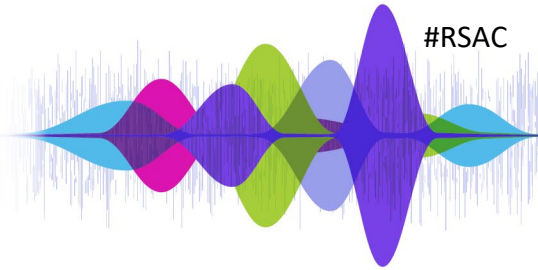
Brain Processes Currently Studied

- Attention
- Fatigue
- Blood flow to specific parts of the brain (measures emotional response/recognition)
- Suggested body movement
- Suggested word generation
- Word and concept recognition
- Dream incubation

Brain Access Devices Currently in Use

- Headband
- Hat
- Wristband
- Earbuds
- Glasses
- Direct Brain-Computer Interfaces
  - Sensor pad placed under skull
  - Wire sunk directly into brain
  - Wire threaded up through jugular vein

EU Report on Neural Privacy



- TechDispatch on Neurodata
  - Neural rights proposed

    1. **Cognitive liberty.** The freedom of a person to decide whether their brain activity and mental processes can be recorded and/or modulated or not.

    2. **Mental privacy.** The freedom and capacity of a person to conceal their mental information and to prevent non-consented intrusion into their cognitive domain.

    3. **Mental integrity.** The prohibition of non-consensual and harmful modulation of a person's neural activity (e.g. malicious brain hacking).

    4. **Psychological continuity.** The right to preserve one's personal identity and continuity of one's mental life from non-consensual external alteration by third parties.

    5. **Fair access.** The ability to ensure that the benefits of improvements to sensory and mental capacity through neurotechnology are distributed justly in the population.

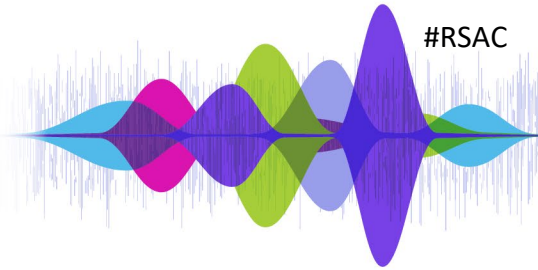
EU Report on Neural Privacy

- TechDispatch on Neurodata
  - Neuro data gathering tools are "very intrusive"
  - Info gathered from your brain is "a special category of data"
    - May provide "deep insights into people's brain activity and reveal the most intimate personal thoughts and feelings, including those that do not translate into actions and consequently cannot be measured or inferred by data collected through other technologies."
    - Subject to heightened requirements under GDPR
  - "Uses of neurodata pose unacceptable risks to fundamental rights and are likely unlawful under EU law"
    - Recording brain activity and manipulating brain activity
    - Immediate or remote
    - Active or passive collection

EU Report on Neural Privacy

- Beyond sensitive data
- GDPR: data controllers must disclose:
  - How neural data is processed and
  - The potential implications to data subjects

Colorado Neural Privacy Law



Extends its omnibus privacy act to include neurological issues in two ways:

- As neural data, which is regulated as sensitive data just by being collected, and
- As biological data (including neural components) with its essentially biometric measurements

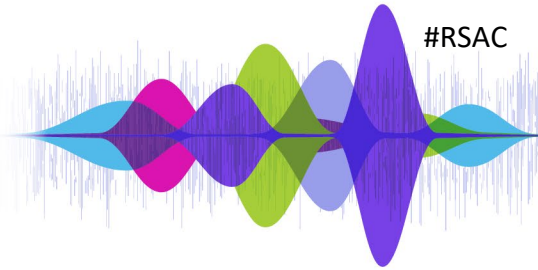
Neural data is "information that is generated by the measurement of the activity of an individual's central or peripheral nervous systems and that can be processed by or with the assistance of a device."

- Can be measured from the head or at any point on the body
- Could measure blood flow, electrical signals, or attention

Neural-based biological data

- As sensitive data, neural data is a subtype of biological data: "data generated by the technological processing, measurement, or analysis of an individual's ... neural properties ... which data is used or intended to be used ... for identification purposes."
- Biological data regulated when collected for identification purposes

California Neural Privacy Extension



- Law extends existing privacy rights to a person's neural data
  - **Neural data** defined as "information that is generated by measuring the activity of a consumer's central or peripheral nervous system, and that is not inferred from nonneural information"
  - Adds neural data to definition of **"sensitive personal information"**
    - Companies must gain permission to use
    - Data subjects may demand deletion and opt-out of any collection regime

Apply to Practice

- Watch for capture of neural information
- Treat it as (at least) sensitive personal data
- Beware of **creepiness** factor

Topic 6:
Software Supply Chain Compromises

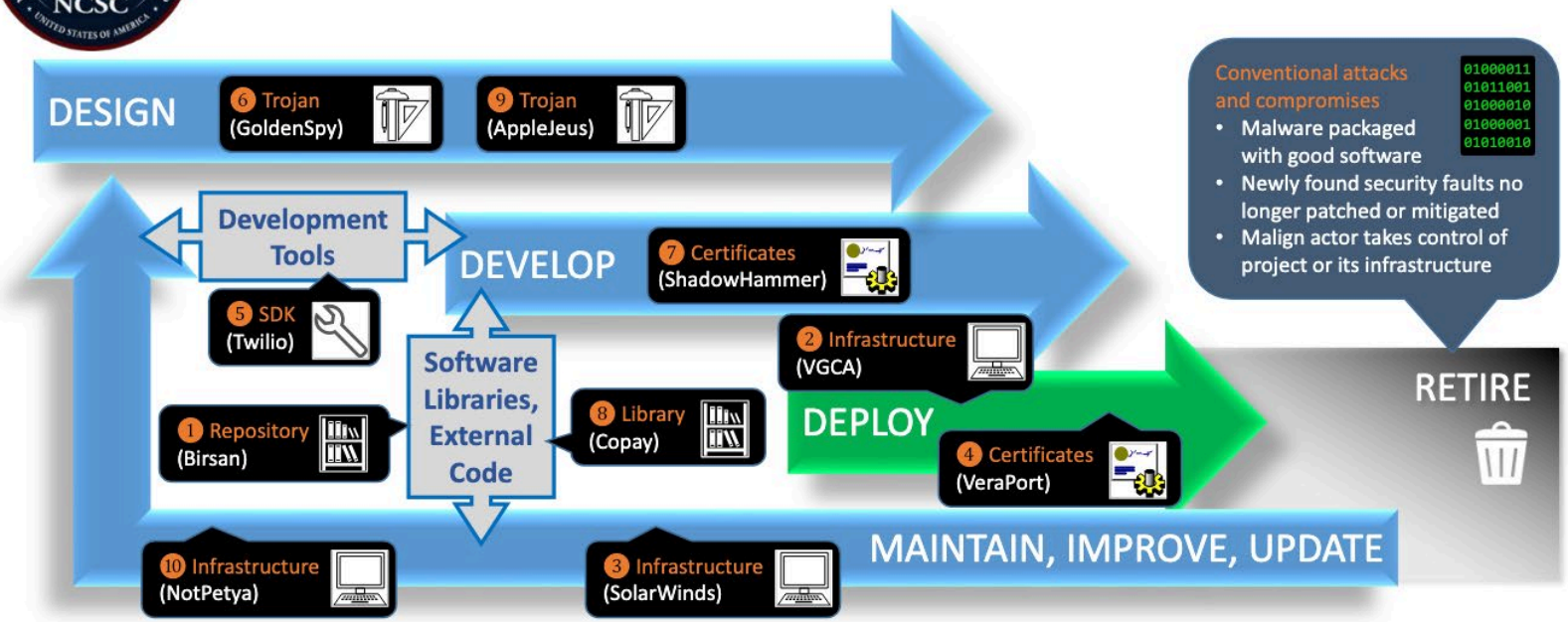
Zero day attacks **exploited vulnerabilities/ flaws in technology used by law firms** as part of their IT operations: e-mail transfer of large files, website transactions, and management of computer networks.

- **Software Development Processes Hijacked:** SolarWinds
- **Software for Secure Transfer of Large Files:** MOVEit; Accellion; Microsoft Exchange Server; Kaseya VSA Ransomware Attack; Apache Log4j
- **Client Data Posted on the Dark Web**
- **Justice Department and FBI Move to Disrupt Hacking Activity (Microsoft)**

Flawed Software Update – Massive IT Outage

Software Supply Chain Attacks

Definition: Compromising software through cyber attacks, insider threats, or other malign activities at any stage throughout its entire lifecycle.



Software Supply Chain Attacks can target products at any stage of the development lifecycle to achieve access, conduct espionage, and enable sabotage.

- Software supply chain attacks can use simple deception techniques such as disguising malware as legitimate products, or use complex means to access and modify the source code of genuine programs.
- Adversaries may seek to exploit tools, dependencies, shared libraries, and third-party code in addition to compromising the personnel and infrastructure of developers and distributors.
- Using software after it reaches end-of-life increases exposure to conventional cyber attacks.

https://www.dni.gov/files/NCSC/documents/supplychain/Software_Supply_Chain_Attacks.pdf

Software Supply Chain Compromises

- Cybersecurity attacks can **expose attorneys to third-party liability**
- **Data breach lawsuit settlements**
  - Gunster $8.5 million (Florida)
  - Orrick $8 million (California)
  - Bryan Cave $750,000 (Illinois)

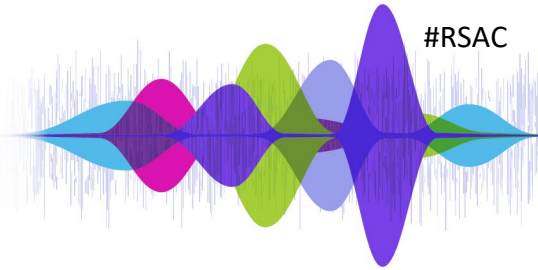
Joint Alert

UK, Canada, New Zealand, US

Protecting Against Cyber Threats to Managed Service Providers and Their Customers

May 11, 2022 – Alert AA22-131A
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-131a

Apply to Practice



- Think holistically about the risk of sophisticated cyber attacks and ransomware (critical for both law firms and clients)
- Take stock of the software and services they rely on
- Hold software vendors accountable for the security outcomes of their products

Topic 7: Cyber Post-*Chevron*

- U.S. Supreme Court's 2024 decisions:
  - *Loper Bright Enterprises v. Raimondo*
  - *Relentless v. Department of Commerce*
- Overturned the longstanding doctrine of **"Chevron"** deference to agency interpretation of ambiguous laws

Cyber Post-*Chevron*

- Impacts on U.S. firm's duties to disclose a cyberattack:
  - Biden-era cyber incident reporting rules for **critical infrastructure**
  - **SEC** enforcement of the 1934 Securities Exchange Act against cybersecurity controls
  - Past **FTC** efforts to finalize regulations on commercial surveillance and data security

Cyber Post-*Chevron*

Impacts under the current Presidential Administration

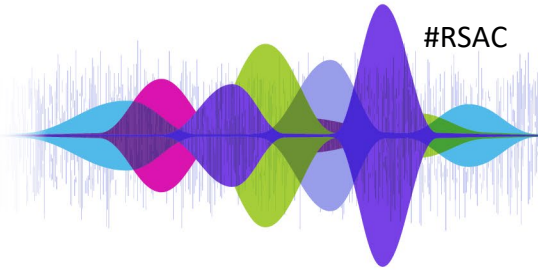
President Trump has retained 3 important Biden-era cybersecurity-related EOs:

Executive Order 14028	Executive Order 14117	Executive Order 14144
Improving the Nation's Cybersecurity	Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern	Strengthening and Promoting Innovation in the Nation's Cybersecurity

Apply to Practice

- Post-Chevron, AI regulation and enforcement domestically are in flux (with little indication this will change in the near term)
- But expect continued support for rules to strengthen federal government and contractors' data security posture, mitigate cyber risk

Topic 8: Takeaways/Apply to Practice



- With great **power** comes great **responsibility**.
  - Just because you can engage in widespread "commercial surveillance" doesn't mean you should. Laws and perceptions are rapidly changing, and you can be tried in the court of public opinion even if what you're doing is legal.
  - Take the surprise out of your practices. Beware of **creepiness** factor. Know your data practices and disclose them.
  - Do what you say (keep your promises, including those about protecting data).
- **AI**
  - Advances in AI have spurred state law to increasingly protect both personal representations (name, image, likeness) and neural 🧠 privacy.
  - Regulatory/enforcement scrutiny might continue, depending on consumer impact and nature of the claims.
  - Follow the NIST *AI Risk Management Framework* to evaluate AI and supply chain risks.
- **Hold software vendors accountable** for the security outcomes of their products.
- **Stay up to date** on the continually evolving legal and regulatory landscape (including lawsuits) in the US and globally AND on the technology driving the legal issues. Check out these **RESOURCES** …

RSAC 2025 Conference

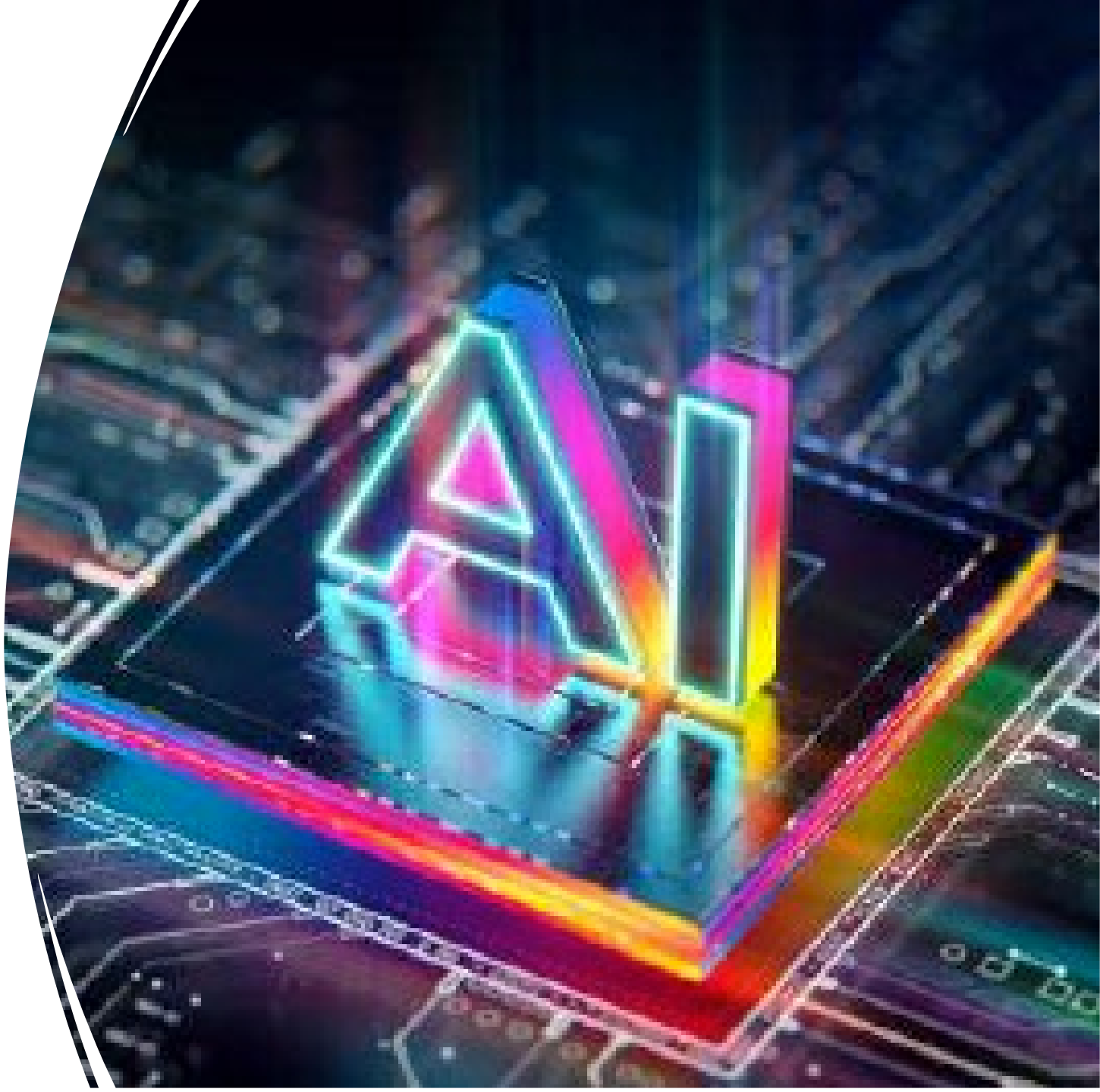
Many Voices.
One Community.

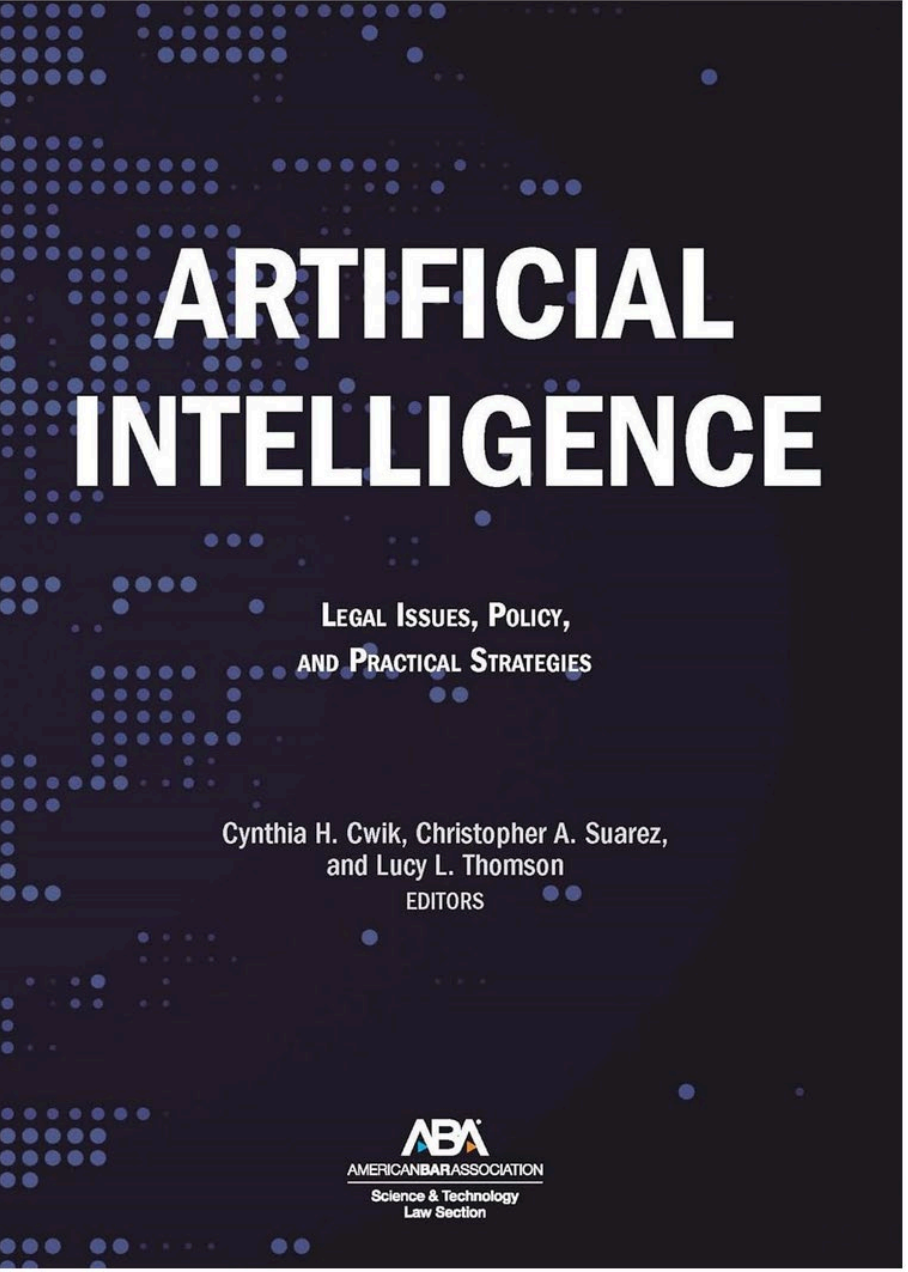
Resources

American Bar Association Task Force on Law and Artificial Intelligence

Year I Report on the Impact of AI on the Practice of Law (2024)
ambar.org/aiLaw

- Law Practice and Ethical Dilemmas
- AI and the Courts
- Access to Justice
- Legal Education
- Governance
- Trustworthy and Responsible AI/Risk Management



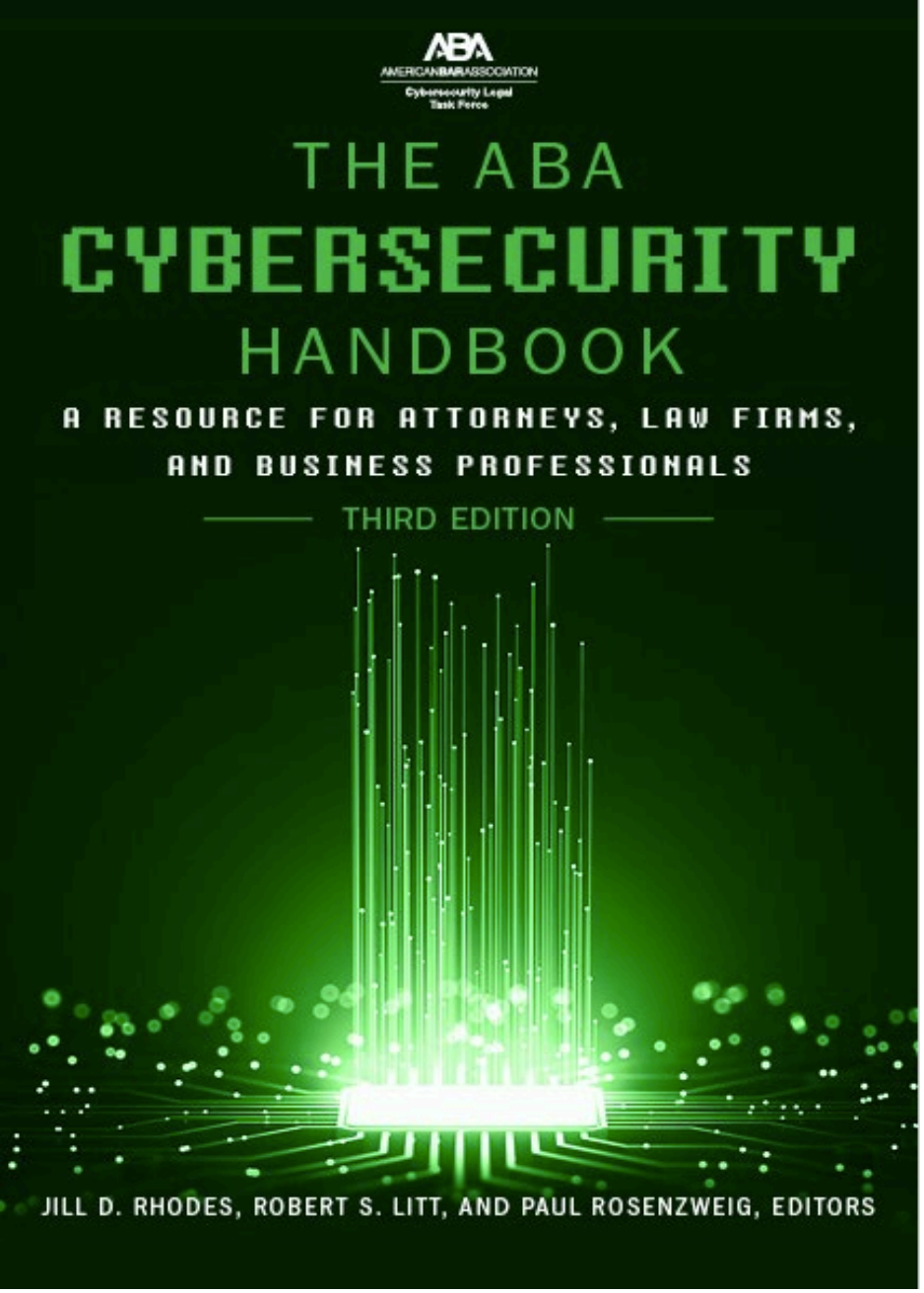


AI is rapidly transforming our world and the practice of law. AI will improve many aspects of legal practice, but it also presents significant challenges. This 2024 book:

- Contains reflections and chapters by over 40 preeminent AI and legal experts from in-house legal departments, private practice, academia, government, and the judiciary.
- Covers a wide range of important topics concerning AI and the law, including the need to protect confidential client information, ensure accurate outputs, and mitigate privacy, security, and IP risks.
- Provides practical advice on how to navigate this complex and rapidly evolving technology.

Get 20% off through 5/20/25 with code SPTNCI20.

Order at ambar.org/aibook



#RSAC

Recognizing the growing volume and sophistication of cyberattacks, *The ABA Cybersecurity Handbook* addresses the current overarching cyber threats, describes how the technology works, outlines key legal requirements and ethical issues, and highlights special considerations for lawyers and practitioners of all types.

From the ABA Cybersecurity Legal Task Force (**ambar.org/cyber**), this bestseller has over two dozen contributing authors.

Get 50% off through 6/30/25 with code PETNI50.

Order at ambar.org/cybersecurity

RSAC 2025 Conference

ABA Science & Technology Law Section (SciTech)

SciTech provides leadership on emerging issues at the intersection of law, science, and technology; promotes sound policy and public understanding on such issues; and enhances the professional development of its members. **ambar.org/scitech**

Programs filled with privacy/security issues, including the 7th annual AI and Robotics National Institute, Santa Clara, CA, October 13-14, 2025

3 Divisions, ambar.org/scitechcommittees

- Interdisciplinary (inclu. AI & Robotics);
- Life Sciences;
- Privacy, Security, and Emerging Technology (10 Committees)

SciTech books, ambar.org/scitechbooks (including 7/24 AI book); **get 20% off** all SciTech books through 5/20/25 with code SPTNCI20.

***The SciTech Lawyer* quarterly magazine**

- AI essentials from past issues, at
  - https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2023/tslai/
- "Where Law and Cybersecurity Come Together: The Synergy of SciTech and the RSA Conference," *The SciTech Lawyer, Fall 2024, at*
  - https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2025/fall/

Who Knows What Other Sizzling Hot Cyber Law Topics Will Emerge? Watch This Space.

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank you

Questions?